# NII-SOCSの運用から浮上してきた セキュリティ対策の課題 ～高度化するサイバー攻撃にどう向き合うか～

高倉弘喜
国立情報学研究所

# NII-Security Operation Collaboration Services(NII-SOCS)の経緯

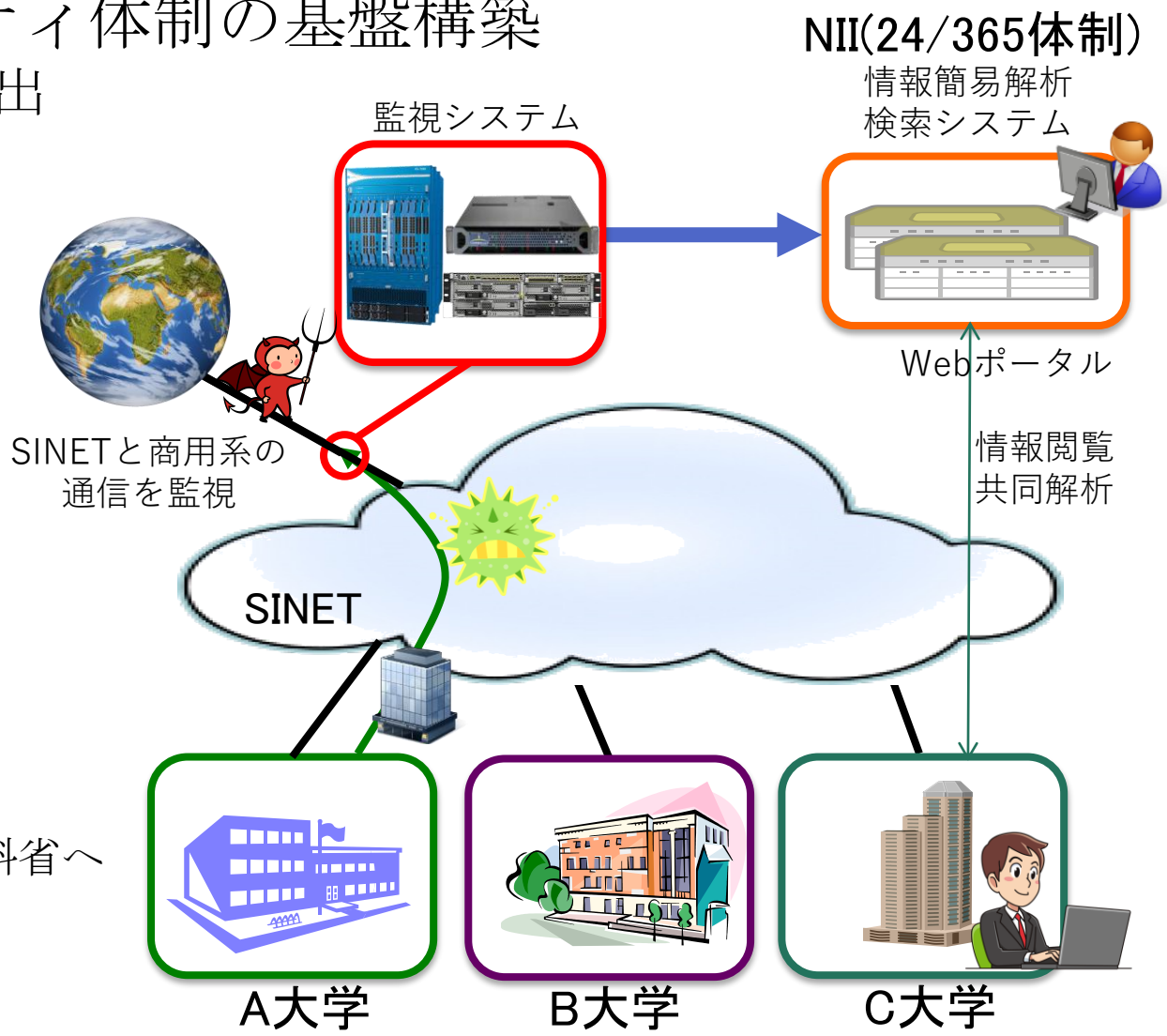
## ■サイバーセキュリティ基本法

- **第八条**　大学その他の教育研究機関は、基本理念にのっとり、自主的かつ積極的にサイバーセキュリティの確保、サイバーセキュリティに係る人材の育成並びにサイバーセキュリティに関する研究及びその成果の普及に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。
- **第三十二条**　本部は、その所掌事務を遂行するため必要があると認めるときは…国立大学法人の学長、大学共同利用機関法人の機構長…に対して、サイバーセキュリティに対する脅威による被害の拡大を防止し、及び当該被害からの迅速な復旧を図るために国と連携して行う措置その他のサイバーセキュリティに関する対策に関し必要な資料の提出、意見の開陳、説明その他の協力を求めることができる。

…と言われても…

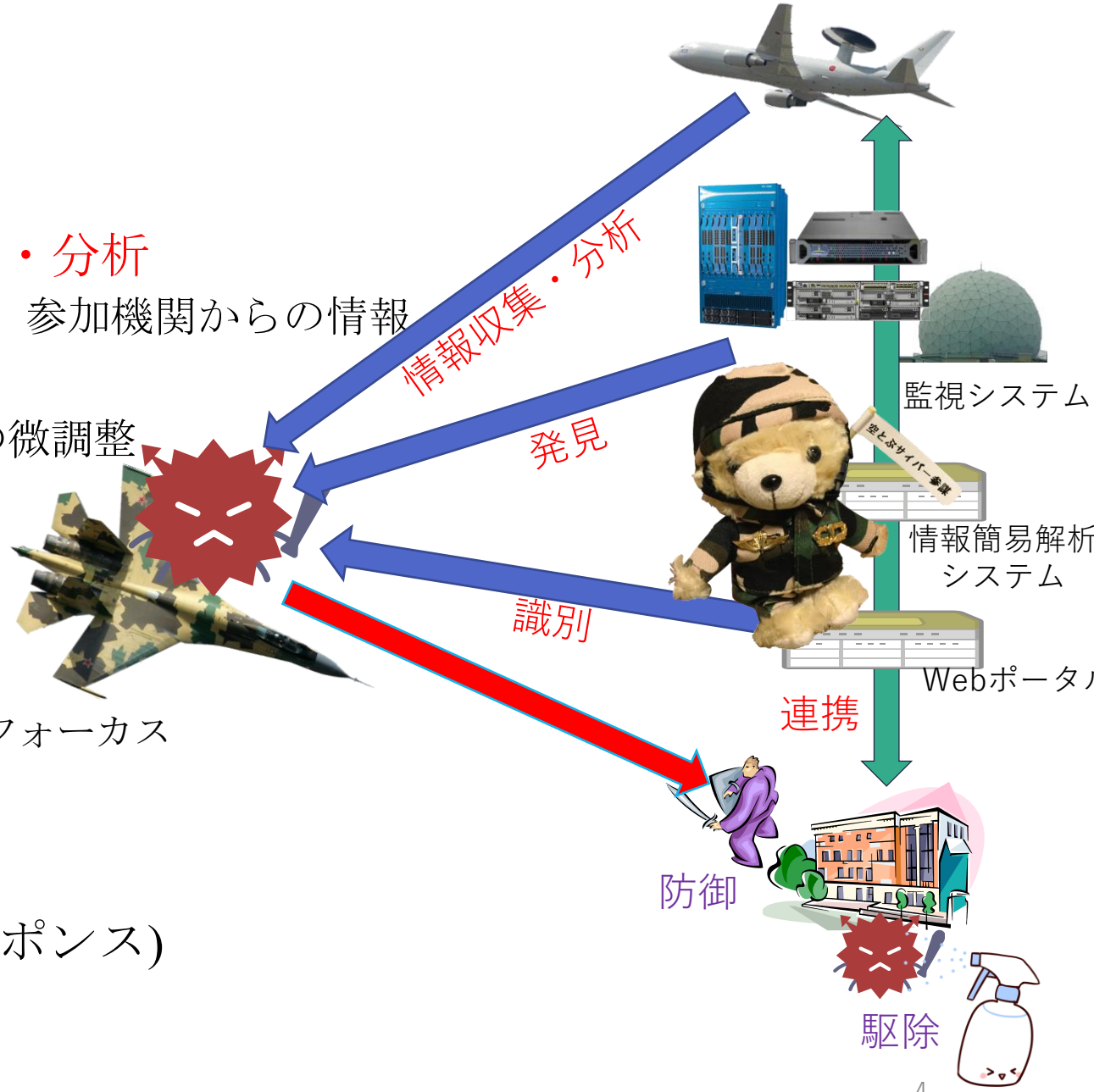
# NII-SOCSの構築と運用

- 大学間連携に基づく情報セキュリティ体制の基盤構築
  - 国立大学法人等の運営費交付金から拠出
    - 7.8億(2016)、8億(2017)、8億(2018)
      - 2021までは継続の予定
  - 3種類の監視システム
    - Sandbox搭載IDS (paloalto)
    - シグネチャベースIDS (Cisco FirePower)
    - DNSトラフィック監視 (Damballa CSP)
  - 簡易解析システム＋Webポータル
    - 膨大な警報に緊急度・危険度の割付
  - 外部セキュリティ機関との情報共有
    - 国内：NDAに基づく攻撃情報の提供
      - サイバー攻撃拠点のNIIへの事前通知
      - NIIは通信の有無のみを回答
        - セキュリティ機関：NISC経由で文科省へ
        - NII：大学に直接通知
    - 海外：MoUに基づく技術情報の共有



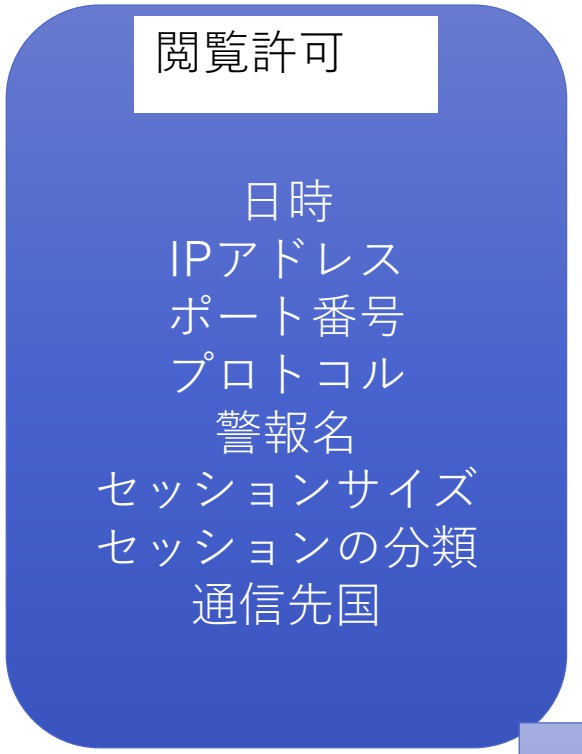
# NII-SOCSの作業の流れ

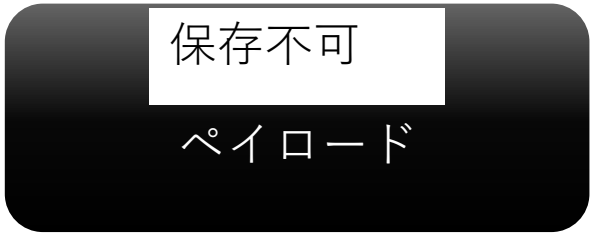
- サイバー攻撃への初動対応
  - 早期警戒情報(インディケータ)の収集・分析
    - 国内・国外のセキュリティ機関、民間、参加機関からの情報
  - サイバー攻撃の発見
    - IDS、サンドボックス、ハニーポットの微調整
  - サイバー攻撃の目標と脅威度の識別
    - 各種情報との照合
    - 攻撃先の分布状況や攻撃手法の解析
    - 被害推定
      - Zero Day攻撃など被害が大きいものにフォーカス
  - 参加機関と連携
- 参加機関
  - 現場対応(予防措置/インシデントレスポンス)
    - 防御や駆除

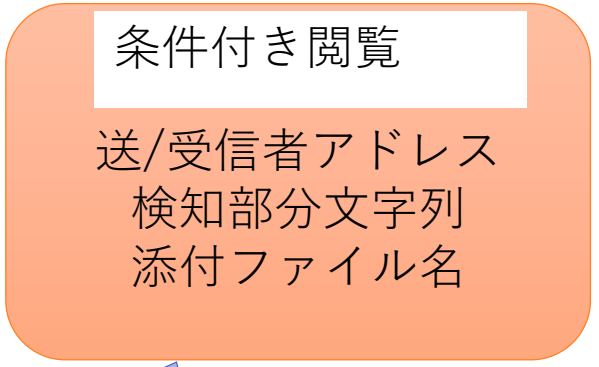


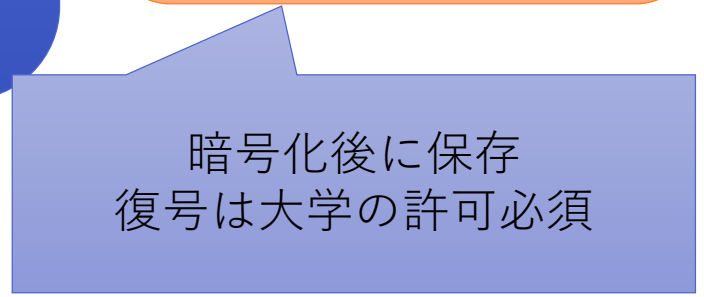
# NII-SOCSの制限

- NIIは大学共同利用機関法人…国に準ずる独法
- 大学の構成員
  - 教職員…国立大学なら公務員に準ずる…
  - 学生・訪問研究者
  - 研究を覗き見るのは…
  - そもそも個人所有の情報端末
- 憲法遵守はmust
  - 通信の秘密
    - 通信の中身は覗けない
  - 財産権
    - 無断の脆弱性診断・コマンド実行不可
- 通信の内容を確認せずに攻撃成否を判断
  - 攻撃着弾後の挙動から推測
    - 誤判定の要因の一つ



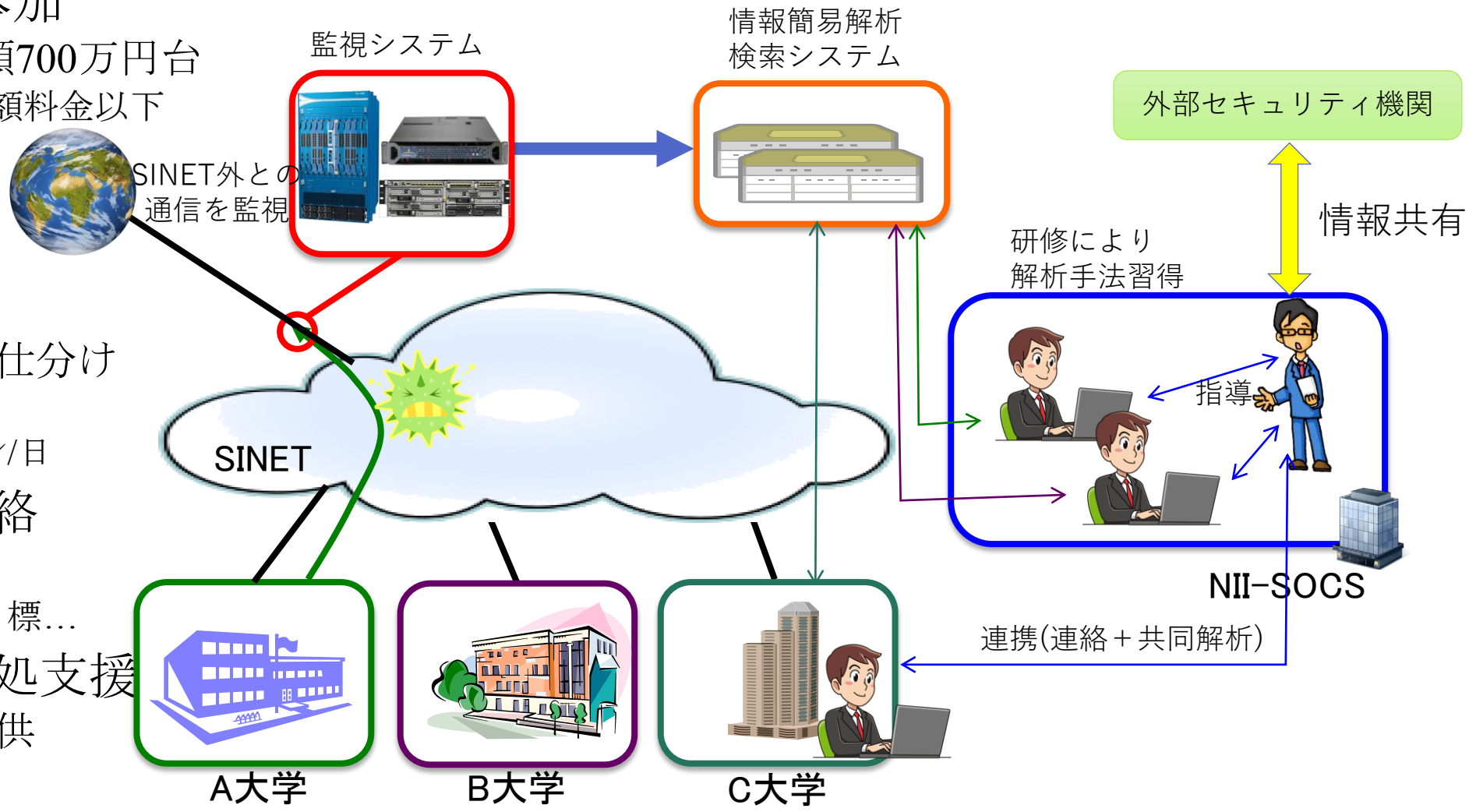



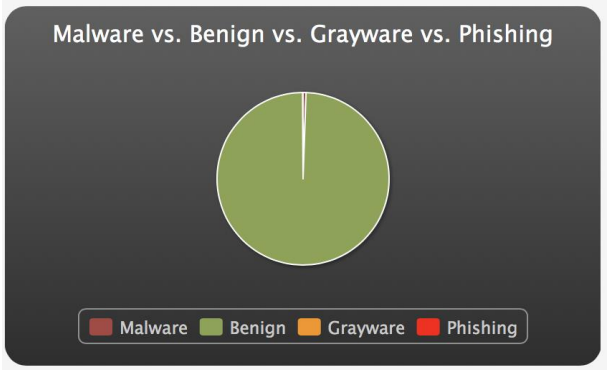
# NII-SOCSの仕組み

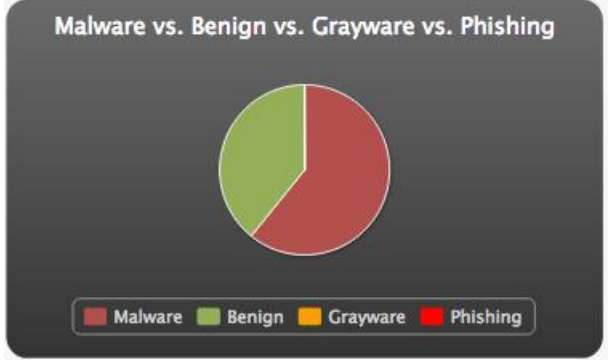
- 100機関以上の参加
  - 1機関あたり年額700万円台
    - 大手SOCの月額料金以下
- 警報監視
  - 24/365体制
    - 平日日中4人
    - 夜間休日2名
  - 簡易解析結果の仕分け
    - 60万警報/日
    - 6億セッション/日
- インシデント連絡
  - 大学へ連絡
    - 週1件程度を目標…
- アクシデント対処支援
  - 必要な情報の提供



# NII-SOCSの運用実績

- いかに絞り込むか?
  - 膨大なデータ
    - 60万警報/日
    - 6億セッション/日
- 概ね30分以内の通知
- 9割を占める
  - マルウェア系
    - 半自動処理
- 残り1割
  - 絞り込み
  - 目視による監視




| 中項目 | | 累計 (2018/4/1~9月末) |
|---|---|---|
| 通知件数 | | 3617 |
| | 分類１：マルウェア感染の可能性 | 2760 |
| | 分類２：アプリケーションソフトの脆弱性によるもの | 225 |
| | 分類３：C&Cサーバーとの実通信の可能性 | 480 |
| | 分類４：ブルートフォース攻撃の可能性 | 0 |
| | 分類５：辞書攻撃の可能性 | 0 |
| | 分類６：標的型サーバー攻撃に関与している可能性 | 0 |
| | 分類７：man-in-the-middle 攻撃 | 0 |
| | 分類８：DNS Amp 攻撃への参加 | 0 |
| | 分類９：その他 | 152 |
| 誤報件数 | | 2 |

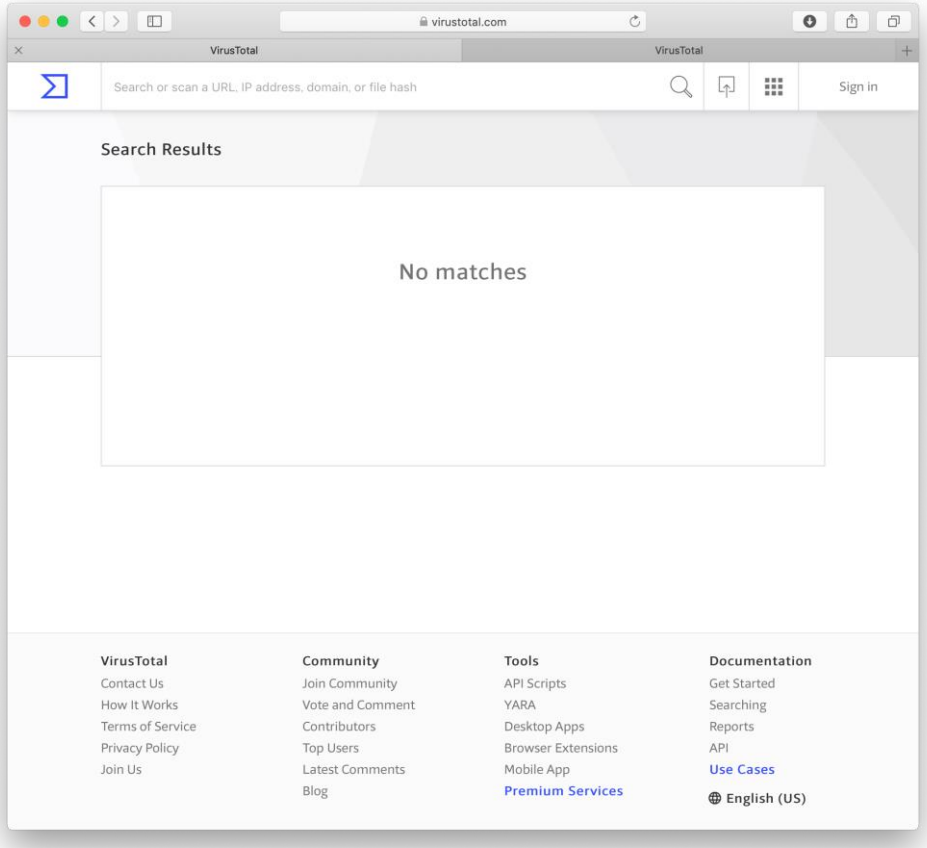
# 挙動の違いによる被害推定

- 追加ダウンロードの可能性あり
  - 関係機関へ通知

| Date | Src IP | Dst IP | Src Port | Dst Port | Protocol | Sent(byte) | Rec. (byte) | Src Country | Dst Country |
|---|---|---|---|---|---|---|---|---|---|
| 2018/5/◯ 09:19:28 | A.B.C.D | W.X.Y.Z | 49940 | 80 | tcp | 2283 | 353460 | Japan | Russian Federation |
| 2018/5/◯ 18:26:14 | E.F.G.H | W.X.Y.Z | 64464 | 80 | tcp | 1154 | 23532 | Japan | Russian Federation |
| 2018/5/◯ 19:07:37 | E.F.G.H | W.X.Y.Z | 50368 | 80 | tcp | 1154 | 23532 | Japan | Russian Federation |
| 2018/5/◯ 16:53:14 | E.F.G.H | W.X.Y.Z | 58072 | 80 | tcp | 1154 | 23532 | Japan | Russian Federation |
| 2018/5/◯ 17:45:15 | E.F.G.H | W.X.Y.Z | 61838 | 80 | tcp | 1154 | 23532 | Japan | Russian Federation |
| 2018/5/◯ 18:15:39 | E.F.G.H | W.X.Y.Z | 64279 | 80 | tcp | 1154 | 23532 | Japan | Russian Federation |
| 2018/5/◯ 19:59:12 | E.F.G.H | W.X.Y.Z | 53316 | 80 | tcp | 1154 | 23532 | Japan | Russian Federation |
| 2018/5/◯ 16:41:48 | E.F.G.H | W.X.Y.Z | 57399 | 80 | tcp | 307 | 14466 | Japan | Russian Federation |
| 2018/5/◯ 18:04:36 | I.J.K.L | W.X.Y.Z | 63829 | 80 | tcp | 307 | 14466 | Japan | Russian Federation |
| 2018/5/◯ 19:37:44 | I.J.K.L | W.X.Y.Z | 52110 | 80 | tcp | 307 | 14466 | Japan | Russian Federation |

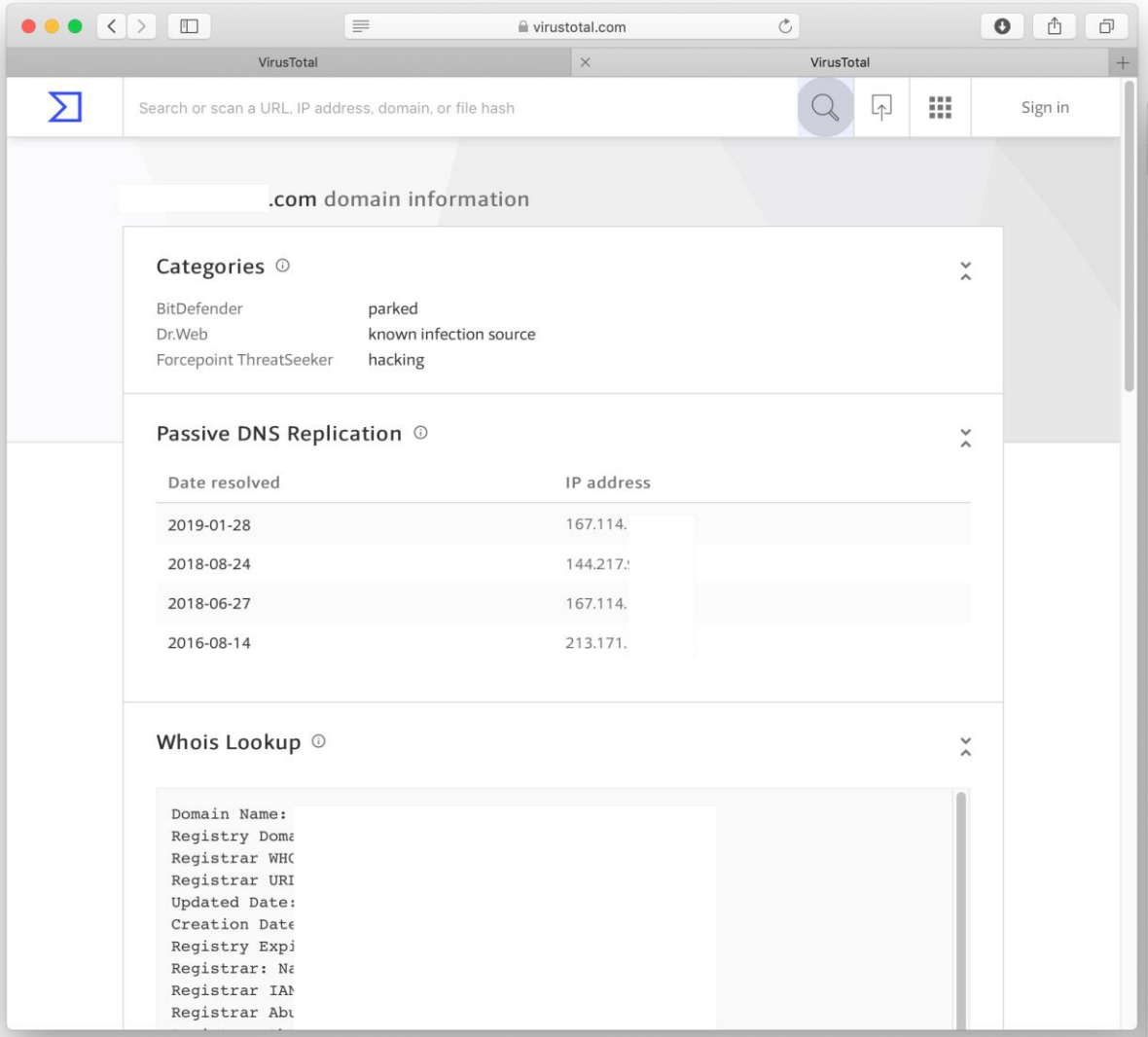
# NII-SOCSの運用方針

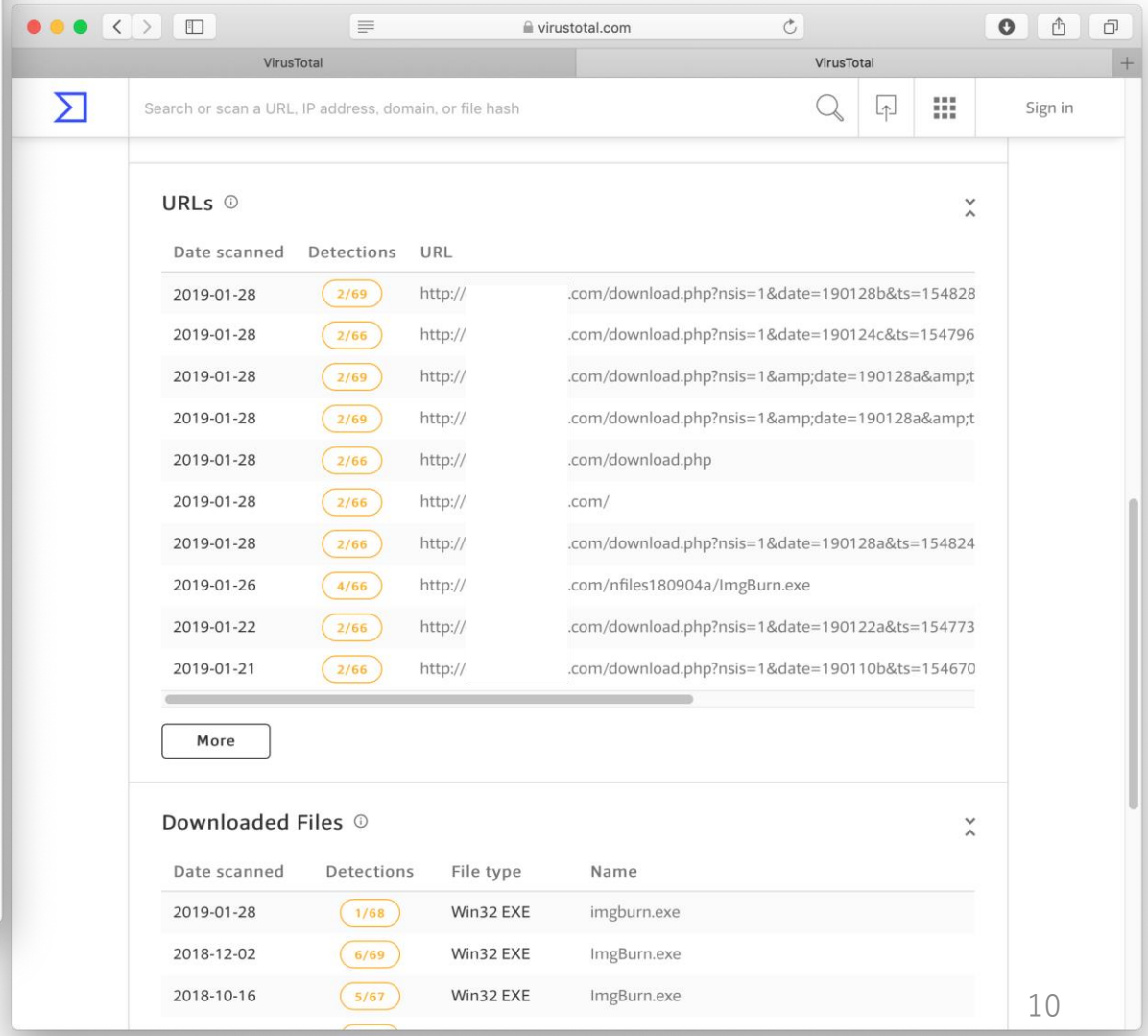
- 最近の攻撃のみ監視
  - 古い脆弱性を狙った攻撃
    - 情報収集目的での検知
      - 古い攻撃の大量発生→未知攻撃の可能性
- マルウェア
  - Sandboxによる検知
    - 通知は大手セキュリティソフト未検知のもののみ
      - 伝えられるのはハッシュ値のみ
      - 来年度からはマルウェア検体の提供も開始するが…
        - 懸念されるVirusTotalへの脊髄反射upload
- よくある誤対応
  - セキュリティソフトで検知されませんでした
    - それは当然
  - なので被害なしと判断します
    - それは大丈夫か？




一定期間経過観察
異常検知→再通知

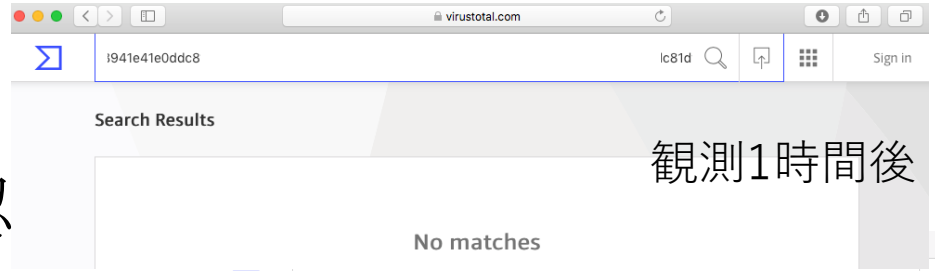
# 配布元ドメインを調べれば疑わしいのは一目で分かるのに…

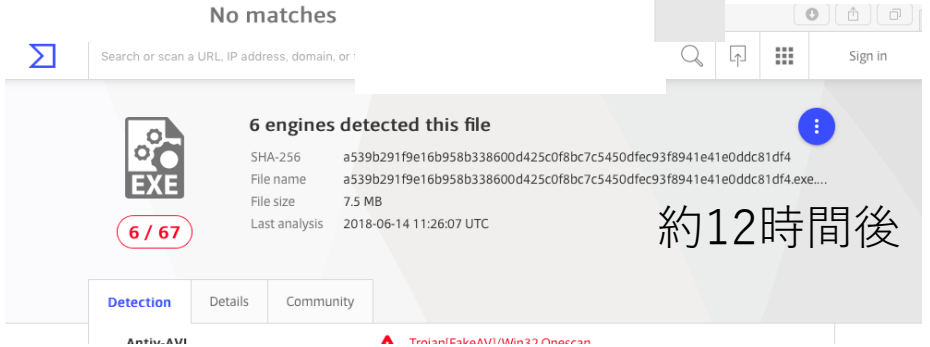


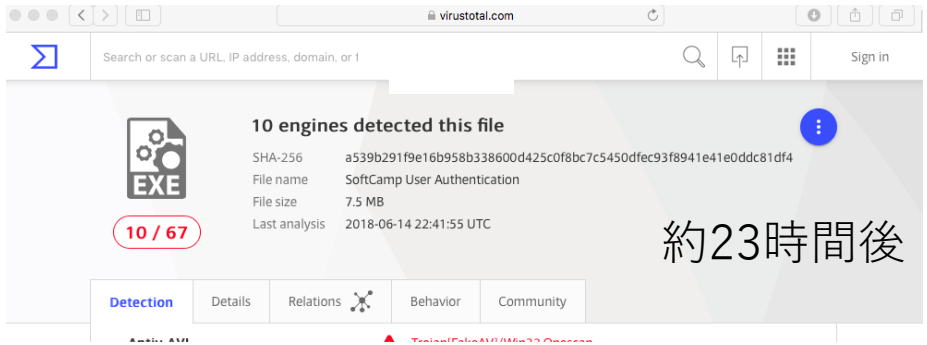



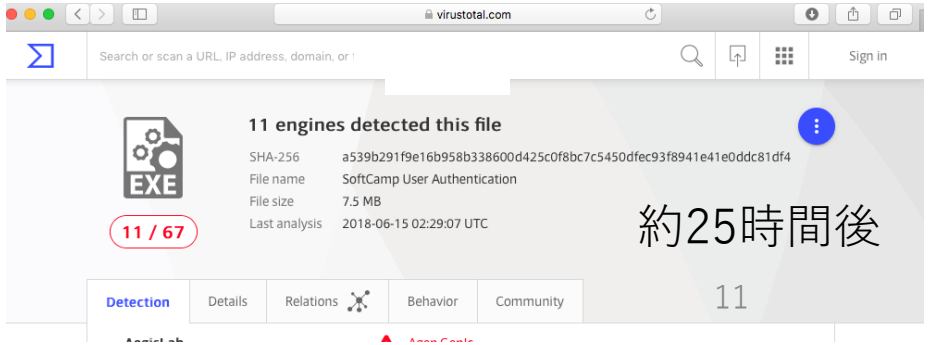
# 標的型攻撃への事例

- NII-SOCSで数名にのみ着弾確認
  - 月に数度は観測
- 採取時は未知マルウェア
  - 検知AV 0は当たり前
    - そもそもサンプルとして上がっていない
- 半日程度で検知が始まるが…
  - サンプルファイルを提供したのは誰か？
    - サンプルがなければ検知パターンが作れない
- 遅々として向上しない検知カバー率
  - 1件のみのサンプル提供
  - 各社サンドボックスからのアクセス回避
    - 緊急度と悪性度の判断しにくい



# IT依存度が急速に高まる大学

- 見えない攻撃にどう対処するのか？
  - 重要なのはインシデント対応、それとも、事業継続？
- CIAからAICへ
  - 大学の事業が継続できること(Availability)
    - そもそもインシデントによるシステム停止と故障によるシステム停止の違いは？
    - 重要システムの故障でも事業継続… ダメージコントロール
  - 情報が得られることも重要(Integrity)
    - 異常データを吐く機器が特定可能
      - データ破棄 or 参考値として使える デグレーテッドオペレーションの可能性
        - NWは生きていることが分かる…も情報
  - 個々の機器のconfidentialityはそこそこでよい

レジリエントな情報システムの設計

# CIAのために事前に立案する要領･手順

- 情報システム単体ではなく業務単位で事前に考えておく
  - アクシデントに至った状況下での適切な判断は困難
    - エリートパニックによる思考停止→全面遮断
- ダメージコントロールを想定した業務体制
  - ある温度センサーでマルウェア感染
  - コントローラでマルウェア感染
  - 認証システムへの不正アクセス

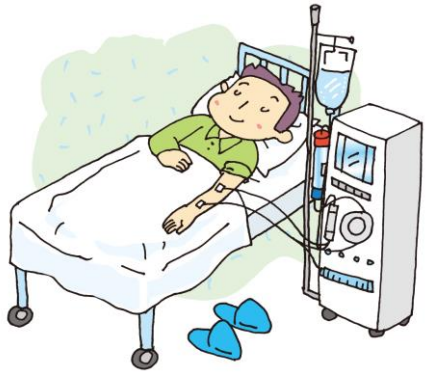
リスクレベルに応じた対応

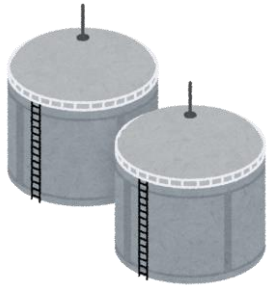
- デグレーデッドオペレーション(縮退運転)を検討
  - 止められない
  - 止めたくない
  - 止めるしかない

停止による影響を考慮

# 止められない情報システム

- 運用停止による影響が甚大
  - 人命に関わるもの(医療機器、危険物の管理)
    - 手動操作が困難
- ダメージコントロール
  - 運用継続による被害拡大防止
    - 防衛ラインの設定(Standalone運用は可能か)
- デグレーデッドオペレーション
  - サイバー攻撃による異常動作も想定
    - 担当者が張り付いてでも運用
    - 後で巻き戻し作業が入っても業務継続
    - 緊急停止機能の確認
    - 代替手段の確保





判断基準・手順のマニュアル化

# 止めたくない情報システム

- 運用停止による影響大
  - 顧客サービス
- ダメージコントロール
  - システム停止の影響範囲を極小化
- デグレーデッドオペレーション
  - 情報システム停止も想定
    - 手動による業務継続
      - 手書き出席票
    - 情報取得を諦めるのもアリ
      - 無料開放

利用者の不利益回避


TOP > セキュリティ > サンフランシスコ市交通局、ランサムウエア攻撃を受けて地下鉄を...

セキュリティ

関連カテゴリー： マネジメント

**サンフランシスコ市交通局、ランサムウエア攻撃を受けて地下鉄を無料に**

2016/12/01

シェア 0 ツイート

John Ribeiro IDG News Service

同交通局のシステムがランサムウエアの攻撃を受けたのは11月25日からだった。報道によると、駅に設置されたコンピューターの画面には、「You Hacked, ALL Data Encrypted（お前をハッキングし、すべてのデータを暗号化した）」というメッセージが表示された。

交通局は、パートナー企業の米Cubic Transportation Systemsの協力のもと、念のための措置として、市営地下鉄の駅で券売機と自動改札口を11月25日から27日朝まで停止した。結果的に、この間は無料で地下鉄に乗ることができた。

http://www.dailymail.co.uk/news/article-2194960/United-Airlines-Computers-passengers-given-handwritten-boarding-passes.html
https://tech.nikkeibp.co.jp/it/atcl/idg/14/481709/120100278/?ST=cio-security&P=2

# 止めるしかない情報システム

- 代替手段がない
- 手動操作は不可能
  - Single Point of Failure(SPF)の存在を把握
    - 経営陣が知っていることが重要
    - 現場判断で停止させないことがベスト
- ダメージコントロール
  - システム停止の影響範囲を極小化
- デグレーデッドオペレーション
  - 多くの場合重要システムなので…

SPFは極力回避


JAL大量欠航を招いた「重量管理」のカラクリ
効率運用の負の側面が顕在化
次ページ »
武政 秀明：東洋経済オンライン副編集長 著者フォロー
2014/06/07 6:00
いいね！ シェア 0 ツイート 一覧 コメント 0 G+ B! 印刷

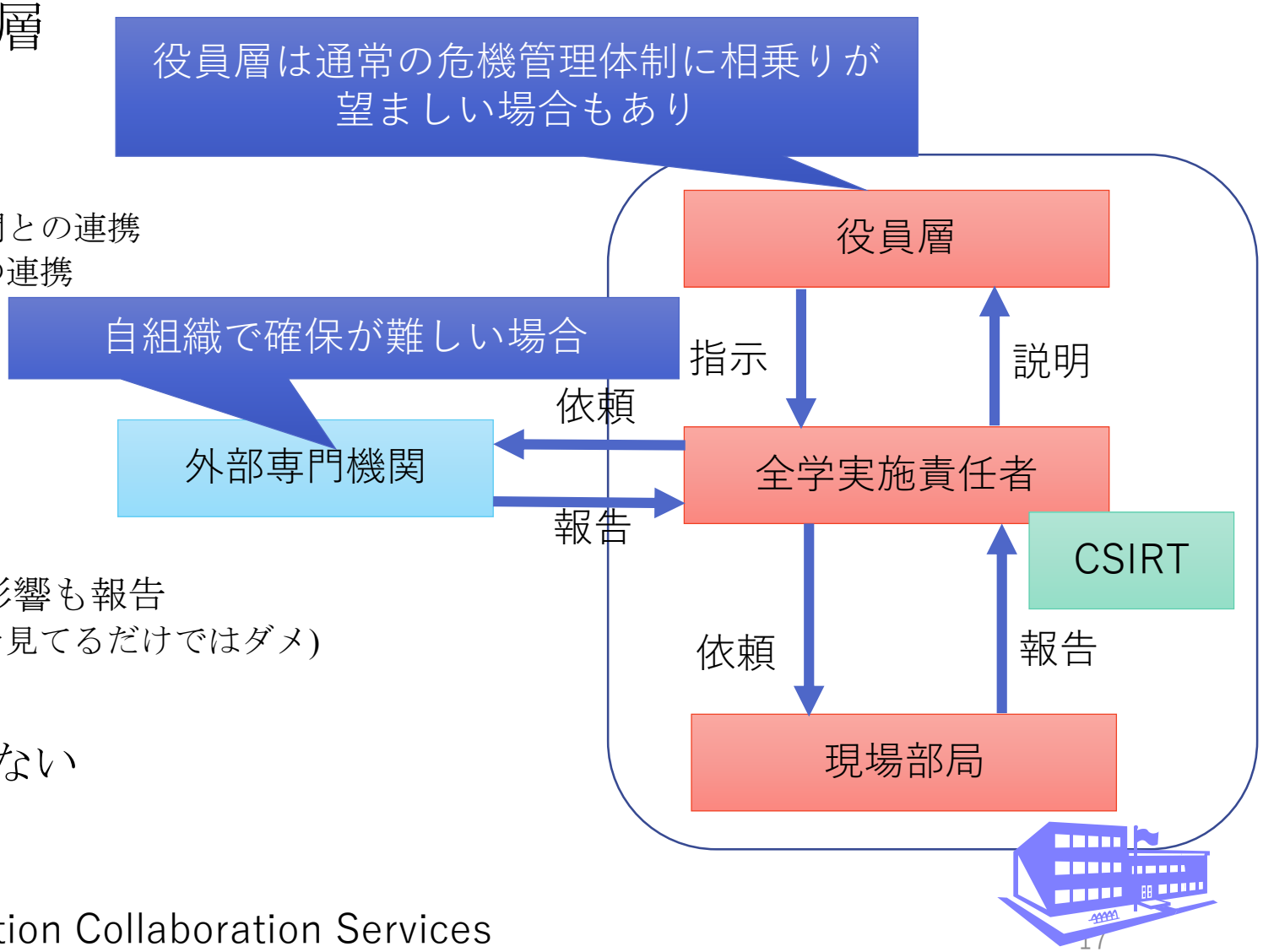

https://toyokeizai.net/articles/-/39544
https://ja.wikipedia.org/wiki/コンテナ#/media/File:Unloading_JAL_747.jpg

# これからの大学に求められる能力

- セキュリティマネージメント層
  - 全学実施責任者
    - 指揮官役としての役割
      - インシデント発生時
        - 外部セキュリティ専門機関との連携
        - インシデント発生現場との連携
        - CSIRTとの調整
        - 役員層-他との意思疎通
      - アクシデント時の判断
        - 事業継続の判断
  - CSIRT
    - 作戦参謀役としての役割
    - 技術だけでなく、組織運営への影響も報告
      - 他部門との連携必須(パソコンを見てるだけではダメ)

自組織での人材育成が必須

- 学内事情に詳しくなければ動けない
- キャリアパスで育成




NII Security Operation Collaboration Services

# 本当に欲しい人材は

- おそらく技術だけのエンジニアは不要となる
  - 今後数年間は…
    - SOCへの外注が進む…次期NII-SOCSの雲行きが…
    - セキュリティマネージメント層
      - ネットワークとセキュリティに詳しくなくてもよい
      - インシデント/アクシデントがBCPに及ぼす規模を想定できることが重要

パソコン触ったことがない人でも務まる…

  - 急速に進むAI化&自動化
    - 雑魚はAIが片付けてくれる
    - 自己免疫機構
      - 攻撃検知と同時に検知パターンや暫定パッチを自動生成
  - それでも残る人による判断
    - 自動対処はあくまでも人が判断する時間を確保するため
    - 暫定パッチ提供の可否・タイミング